

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
11 August 2005 (11.08.2005)

PCT

(10) International Publication Number
WO 2005/073825 A2

(51) International Patent Classification⁷:

G06F

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(21) International Application Number:

PCT/IB2005/050254

(22) International Filing Date: 21 January 2005 (21.01.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04100279.1 27 January 2004 (27.01.2004) EP

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **TIMMERMANNS, Daniel** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agents: **ELEVELD, Koop, J. et al.**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

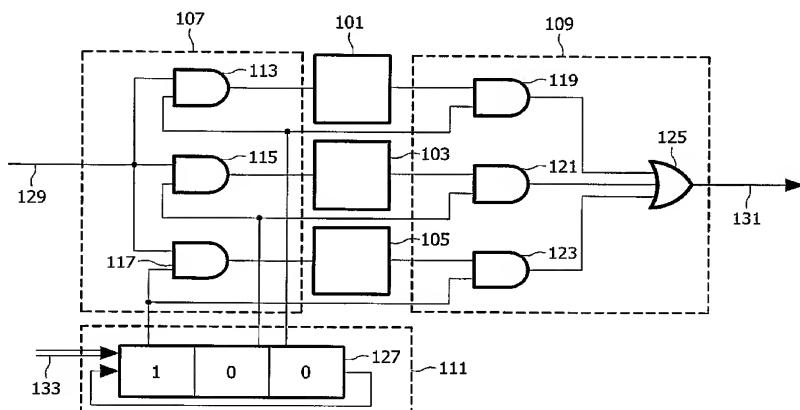
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE,

[Continued on next page]

(54) Title: PROTECTION AGAINST POWER ANALYSIS ATTACKS



WO 2005/073825 A2

(57) Abstract: An electronic circuit for cryptographic processing, comprising a first combinatorial logical circuit, arranged to perform a first set of logical operations on input data and to produce output data, the output data having a functional relation to the input data, further comprising at least a second combinatorial logical circuit, arranged to perform a second set of logical operations on the same input data and to produce output data, the output data having an identical functional relation to the input data, wherein the first set of logical operations is different from the second set of logical operations, and wherein the electronic circuit is arranged to dynamically select one combinatorial logical circuit, of a set comprising at least the first combinatorial logical circuit and the second combinatorial logical circuit, for performing logical operations on the input data and producing output data.



EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS,
JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA,
MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM,
PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY,
TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA,
ZM, ZW. ARIPO patent (BW, GH, GM, KE, LS, MW, MZ,
NA, SD, SL, SZ, TZ, UG, ZM, ZW). Eurasian patent (AM,
AZ, BY, KG, KZ, MD, RU, TJ, TM). European patent (AT,
BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR,
HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK,
TR). OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG)

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.